МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Ярославский государственный университет им. П.Г. Демидова»

Математический факультет

Кафедра компьютерной безопасности

Заведующий кафедрой:

д. ф. - м. н., профессор

Мурин Д. М.

Направление подготовки

10.05.01 Компьютерная безопасность

Курсовая работа

Обнаружение аномальной активности в сети на основе анализа статистических отклонений в работе системы.

Научный руководитель

д. ф. - м. н., доцент

\_\_\_\_\_\_\_\_ Д. А. Савинов

«\_\_» \_\_\_\_\_\_\_\_\_ 2025 г.

Студент группы КБ-41СО

\_\_\_\_\_\_\_\_ А.Ю.Сластухин

«\_\_» \_\_\_\_\_\_\_\_\_ 2025 г.

Ярославль 2024 г.

Оглавление

Оглавление 2

Литература 4

Перехват и обработка сетевого трафика.

Типы сетевых атак. Подходы к их выявлению.

Построение алгоритма выявление небезопасной сетевой активности на основе анализа статистических данных по многим факторам.

Реализация гибкой настройки с добавлением своих данных и выбором параметров для возможности использования в узкоспециализированных системах.

https://selectel.ru/blog/ips-and-ids/

<https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids>

<https://cyberleninka.ru/article/n/obzor-otkrytyh-naborov-dannyh-dlya-vyyavleniya-atak-na-veb-prilozheniya/viewer>

О том, где искать дата сеты

https://habr.com/ru/companies/vasexperts/articles/790192/

Литература

1. <https://habr.com/ru/companies/raiffeisenbank/articles/346380/>
2. <https://habr.com/ru/companies/serverspace/articles/692916/>
3. Эндрю Таненбаум «Современные компьютерные системы» 1992
4. Йоррит Хердер (Jorrit N. Herder), Херберт Бос (Herbert Bos), Эндрью Таненбаум (Andrew S. Tanenbaum) «Построение надёжных операционных систем, допускающих наличие ненадёжных драйверов устройств». Перевод: Сергей Кузнецов. <http://minix3.ru/articles/reliable-os.html>
5. Йоррит Хердер (Jorrit N. Herder), Херберт Бос (Herbert Bos), Эндрью Таненбаум (Andrew S. Tanenbaum) «Модульное программирование в MINIX 3». Перевод: Сергей Кузнецов.   
   <http://minix3.ru/articles/mspinm3.html>
6. <https://ru.wikipedia.org/wiki/MS-DOS>
7. <https://dzen.ru/a/ZEuqclvPyAKVx-nV>
8. <https://ru.wikipedia.org/wiki/История_Linux>
9. <http://minix3.ru/articles/introduction_minix3.html>
10. <https://ru.wikipedia.org/wiki/MINIX_3>

Идеи для реализации

1.Обязательно учесть систему доверенного третьего лица, которое будет реализовывать соответствующий интерфейс.

2.Файловая система – это модуль системы, которых может быть много, это обеспечить высокую пропускную способность, увеличивая нагрузку на сеть

Например: в Mongo DB существуют коллекции, было бы круто равномерно распределить все файлы на несколько «узлов файловых систем», каждый из которых отвечает за свою коллекцию, чтобы можно было параллельно обрабатывать большие потоки данных.

3.Существуют различные системы для хранения файлов на серверах – рассмотреть возможность создания прослойки для работы с такими системами как с будто бы это файловая система нашей машины – это позволит использовать уже существующие решения для создания высокопроизводительной, адаптивной под задачи, системы.

4.Определиться, как рассматривать ОС – пока я представляю ОС как множество сетевых узлов, на которых может быть любая Физическая ОС, подобранная для конкретной функции – т.е. рассматривать ОС как сборку уже готовых решения, на данный момент трудно будет заставить всех перейти на новую структуру

5.В последствии рассмотреть вариант создания своего микроядра, совместимого со всеми аппаратными решениями – это очень сложно(

6.Что делать с графикой? Видеокарта – тоже модуль системы. Полагаю, нужно посылать вычислительные задачи на разные узлы, чтобы успевать обрабатывать запросы графики.

7.Пользовательский компьютер – терминал или очень слабое, в сравнении с системой, устройство для примитивных задач.

8.В данной топологии ОС, которую хочу строить будет мало уязвимостей современных ПК, но не забывать про сетевые атаки – всё взаимодействие идёт по сети, не факт, что локальной.

9.Обязательно систему хранения логов, например, ElasticSearch и системы выявления аномалий(Алгоритмическую и AI)

10.В системе скорее всего будут важные распределительные пункты, они должны быть просты, их цель распределить задачи по распределённым узлам.

11.Поговорить о безопасности(Литература 4 – интересная статья)

12.Сервер реинкарнации – от него порождаются все процессы, он отлавливает подвисшие-зомби процессы, удаляет их, перезапускает и сообщает об этом другим серверам.

13.Возможность склонировать и запустить параллельно уже работающий модуль системы для того, чтобы распараллелить нагрузку или чтобы удобно протестировать без вреда для всей системы.